User Guide

AWS Console Mobile Application

AWS Console Mobile Application: User Guide

Table of Contents

What is the AWS Console Mobile Application?

The AWS Console Mobile Application lets you view and manage a select set of resources and receive important push notifications to stay informed and connected with your AWS resources while on-the-go.

With the Console Mobile Application, you can monitor resources and view configuration details, metrics, and alarms for a select subset of AWS services. You can see an overview of the account status with real-time data on Amazon CloudWatch, AWS Personal Health Dashboard, AWS Billing and Cost Management, and Recently Visited Services. You can view ongoing issues and follow through to the relevant CloudWatch alarm or CloudWatch dashboard screen for a detailed view with graphs and configuration options. In addition, you can check on the status of specific AWS services, view detailed resource screens, and perform some actions.

You can also get instantly notified about resources of interest by using push notifications. Push notifications allow you to get a snapshot of messages or issues and assess the situation without having to log in to the Console Mobile Application. If you want to follow up on a notification, you can choose the notification and upon successful login, be directed to the relevant screen inside the application.

The Console Mobile Application requires an existing AWS account. After you sign in with your user credentials or a federated role, the Console Mobile Application remembers your credentials and securely stores them in your mobile device's password manager so that you can easily switch between identities from the identities screen of the Console Mobile App. You can also use hardware authenticators, such as Yubikeys, for additional security while signing in to your AWS account from the Console Mobile Application.

Accessing the AWS Console Mobile Application

You can download the Console Mobile Application from the iOS App Store, Google Play, Amazon Appstore, or by scanning the following QR code:

Default service quotas for the AWS Console Mobile Application

There are no quotas imposed by the Console Mobile Application, but there may be limitations imposed by the other AWS services that you use on the app. For more information, see AWS Quotas.

Setting up for the AWS Console Mobile Application

Complete the tasks in this section to get set up to use the Console Mobile Application.

Steps

- the section called “Step 1: Sign up for AWS”
- the section called “Step 2: Check system requirements”
- the section called “Step 3: Download the app”

When you’re finished, you will be ready for the Getting started with AWS Console Mobile Application tutorial.

Step 1: Sign up for AWS

If you do not have an AWS account, complete the following steps to create one. Note that this step must be done from the AWS Management Console on your desktop.

To sign up for an AWS account

1. Open https://portal.aws.amazon.com/billing/signup.
2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

Step 2: Check system requirements

Mobile devices

We support iOS 16.4 and above, and Android 8.0 and above.

Tablets

The Console Mobile Application is optimized for iOS and Android mobile devices with a screen size smaller than 7 inches, but it works on larger screen sizes as well.

Step 3: Download the app

Download the Console Mobile Application from the iOS App Store, Google Play, Amazon Appstore, or by scanning the following QR code:

Getting started with the AWS Console Mobile Application

Use this tutorial to get started with the Console Mobile Application. You'll learn about required IAM permissions, how to authenticate through the app, and how to view your AWS resources through the app.

Prerequisites

Before you begin, be sure that you've completed the steps in Setting up for the AWS Console Mobile Application.

To log in to the Console Mobile Application, we recommend using either your user credentials or a federated role, rather than a root account. When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account root user and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you don't use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see Tasks that require root user credentials in the *AWS Account Management Reference Guide*.

To sign in as a user, you need to use either the account number or the account alias, which can be found at the top of the Management Console sign-in screen.

To sign in with a federated role, you need the federation link from your administrator.

If you use AWS Multi-factor Authentication (MFA), we recommend using either a hardware key fob MFA device, a hardware display card MFA device, or a virtual MFA device for the greatest level of account protection. For a list of MFA devices that you can use, see Multi-factor Authentication.

The Console Mobile Application does not currently support using U2F security keys for MFA. For more information, see Supported configurations for using U2F security keys in the *IAM User Guide*.

You can set up biometric authentication on supported iOS and Android devices running the Console Mobile Application version 2.0 and newer.

Step 1: Verify your permissions

To use the Console Mobile Application, you need the same permissions you use to access the AWS Management Console on your desktop. This means you need some basic AWS permissions, in addition to permissions for the AWS services you want to access from the Console Mobile Application.

> **Note**
>
> To use AWS Billing and Cost Management in the Console Mobile Application, you need to have permissions for the AWS Cost Explorer API, rather than for the AWS Billing and Cost Management console.

The following example shows a JSON policy that allows the user to use the AWS Cost Explorer API:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ce:*"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Step 2: Sign in

To sign in as a first time Root or IAM user

1. In the Console Mobile Application, select **Use an AWS identity**.
2. Enter your AWS identity information.
3. (Optional) Enable biometric authentication.

> **Note**
>
> If you have a virtual MFA device or a hardware authenticator enabled for MFA, you will be prompted to enter your MFA code or use your hardware authenticator to verify your identity.

4. Choose **Sign in**.
5. (Optional) Save your password using your password manager.
6. View your home screen.

To sign in for the first time as an IAM Identity Center user

1. Sign in using a QR code:
   a. On your desktop device, navigate to the AWS access portal.
   b. Open the right sidepanel by choosing **More ways to access AWS**.
   c. Use your mobile device to scan the **Access the console in the mobile app** QR code.

   > **Note**
   >
   > If you use an Android device, we recommend using a third-party QR code scanner app or Google Lens to scan the **Access the console in the mobile app** QR code.

2. (Optional) Or sign in using a URL:
   a. In the Console Mobile Application, select **Use a sign in URL**.
   b. Enter your organization's sign in URL. This directs you to your organization's federated sign in page.

   > **Note**
   >
   > If your organization uses IAM Identity Center, when an administrator creates a user in IAM Identity Center on your behalf an email invitation to join IAM Identity Center containing a one-time password and AWS access portal URL is typically sent to you.

3. Enter your organizational credentials (for example, a user name and password).
4. Choose **Sign in**.

5. If you are asked for a verification code, check your email for it. Then enter or paste the code in the sign-in screen.

> **Note**
>
> If you have a virtual MFA device or a hardware authenticator enabled for MFA, you will be prompted to enter your MFA code or use your hardware authenticator to verify your identity.

6. (Optional) Save your password using your password manager. We recommend doing this step.
7. Select an AWS account and role to assume.
8. View your home screen.

To sign in as a first time Federated user

1. In the Console Mobile Application, select **Use a sign in URL**.
2. Enter your organization's sign in URL. This directs you to your organization's federated sign in page.

> **Note**
>
> If your organization uses a federated or third-party identity provider like Windows Active Directory, Okta, or Salesforce Identity, contact your administrator to get your sign in URL.

3. Enter your organizational credentials (for example, a user name and password).
4. Choose **Sign in**.
5. If you are asked for a verification code, check your email for it. Then enter or paste the code in the sign-in screen.

> **Note**
>
> If you have a virtual MFA device or a hardware authenticator enabled for MFA, you will be prompted to enter your MFA code or use your hardware authenticator to verify your identity.

6. (Optional) Save your password using your password manager. We recommend doing this step.

7. Select an AWS account and role to assume.
8. View your home screen.

To sign in as a returning Root, IAM, or Federated user

AWS identities previously used to sign in are listed on the **Identities** screen of the Console Mobile Application. If your AWS identity credentials are saved in your mobile device's password manager, you can auto-fill your credentials for faster sign in. If you have a virtual MFA device or a hardware authenticator enabled for MFA, you will be prompted to enter your MFA code or use your hardware authenticator to verify your identity before signing in.

Step 3: View your home screen

From the home screen, you can view information about CloudWatch alarms, AWS Health, Cost Management, and Recently Visited Services.

View and modify CloudWatch alarms

In the CloudWatch widget you can see the status of your alarms. To see more information about your alarms, you can choose the red number of those in alarm or with insufficient data. This shows you a list of those alarms, which you can search or filter.

You can filter your alarms by choosing **Filter**, then choosing one of the following options:

- In alarm
- OK
- Insufficient data

To view more information about an alarm, choose the alarm you want to view. The alarm detail screen will appear. You can see more information about the alarm status, threshold, and more.

To modify an alarm threshold, choose **Modify**.

View CloudWatch custom dashboards

To view your CloudWatch custom dashboards

1. In the CloudWatch widget on your home screen, choose **View dashboards**. You can then view a list of all of the CloudWatch custom dashboards your AWS identity has access to.
2. Select the CloudWatch custom dashboard that you want to view.
3. (Optional) Adjust the date or timespan to change the viewable data.

View AWS Health details

On the home screen, under **AWS Health**, you can see your open issues past 7 days, your scheduled changes, and other notifications past 7 days. Choose any of these numbers to view more information about these events. To view all of your events, choose **View all**. You can browse and search your event log.

View Cost Management details

To view your Cost Management details, from the home screen, under **Cost Management**, choose your month-to-date costs or **View details**. You can explore your month-to-date costs and more.

View Recently Visited AWS Service details

On your home screen, under **Recently Visited**, you can view a swipeable list of your ten most recently visited AWS services that are supported in the application. These services are listed from most recently visited to least recently visited. Your recently visited AWS services are synchronized between your mobile and web experiences so you can view your recently visted services across platforms.

(Optional) Step 4: Enable push notifications

If you want to receive push notifications about AWS services and resources of interest on your mobile device, enable push notifications. For more information, see Push notifications.

(Optional) Step 5: Access Amazon Q

If you want to receive in-app answers to your AWS service questions, access Amazon Q. You can access the generative Artificial Intelligence (AI) from the Amazon Q tab at the bottom of your screen if you have the necessary permissions. For more information, see What is Amazon Q Developer? and AmazonQFullAccess in the the *Amazon Q User Guide*.

> **Note**
>
> For Apple users, Amazon Q is supported on iOS 16 and higher.

Step 6: View information about other AWS services

At the bottom of the screen, choose the **Services** tab. You will see a list of all of AWS services that are supported in the application.

If any of your services are in alarm, you will see the number of alarms in red.

Choose any service to view more information about that service.

For a list of supported services, see Supported AWS Regions and services.

Step 7: Access AWS CloudShell

The CloudShell tab is at the bottom of the screen. If you choose **CloudShell** and it's available in the AWS Region you've selected, a full screen modal appears and the CloudShell terminal loads for use. You can exit CloudShell at any time by choosing **X**. If you choose **CloudShell** and it isn't available in your selected Region, a dialog appears informing you that CloudShell isn't supported in your currently selected Region. It also lists what Regions CloudShell is available in, should you choose to switch to a supported Region.

For more information about CloudShell Region availability, see AWS Cloudshell endpoints and quotas in the *CloudShell Reference Guide*.

You can download the Console Mobile Application from the iOS App Store, Google Play, Amazon Appstore, or by scanning the following QR code:


aws
Scan to Download

Push notifications

You can use Notifications in the Console Mobile Application to create actionable push notifications from AWS services, such as CloudWatch. These notifications can be delivered to your mobile device when a resource requires your attention. Enabling push notifications requires you to share your device ID with AWS. Use this tutorial to get started with and manage your push notifications in the Console Mobile Application.

> **Note**
>
> Push notifications depend on external services, such as Apple and Google messaging services. In the event of a service outage, AWS can't guarantee the reliability or timeliness of notification delivery.

Prerequisites

Before you begin, be sure that you've completed the steps in Getting started with the AWS Console Mobile Application.

To receive push notifications, you must have the appropriate AWS User Notifications permissions. For more information, see Resource-level permissions in the *AWS User Notifications User Guide*.

Step 1: Get started with push notifications

To receive notifications about resources of interest, you must allow push notifications and create or subscribe to an existing notification configuration. A notification configuration is a container of your selected services and event rules. An event rule specifies what event generates a notification.

To create new notification configurations

1. In the Console Mobile Application, from the tab menu at the bottom of your device, choose **Notifications**.
2. Choose **Agree**.
3. Choose **Allow**.
4. Set up notification configurations as follows:

> **Tip**
>
> If someone in your account has already created notification configurations, you can use them by choosing **Select existing**. For more information, see the next procedure.

a. Choose **Create new**.

b. Enter a name.

c. (Optional) Enter a description.

> **Tip**
>
> Using distinct descriptions helps other account users differentiate alarms.

d. Select a Region.

e. (Optional) Select alarms.

> **Note**
>
> Choosing **Specific alarms** allows you to select individual alarms to receive notifications for. Choosing **All alarms** selects all available alarms in the account. Note that choosing **All alarms** can result in increased notifications.

f. Choose **Next**.

5. View your selected notification configurations.

To select existing notification configurations

1. In the Console Mobile Application, from the tab menu at the bottom of your device, choose **Notifications**.
2. Choose **Agree**.
3. Choose **Allow**.
4. Set up notification configurations as follows:
   a. Choose **Select existing**.
   b. Select notification configurations by choosing the plus sign (**+**).

c. View your selected notification configurations.

> **Note**
>
> You can view other notification configurations by choosing the **All** tab. You can always return and modify previously selected notification preferences from this screen. If you deselect a notification configuration, you won't receive push notifications for it.

Step 2: Viewing notifications

You can view console notifications directly in the Console Mobile Application.

> **Note**
>
> Whenever a new notification is available, the bell icon in the tab menu shows a blue badge. If you log out of the application, you will still receive push notifications on your device. You must sign back in to the application to view its details.

To view your notifications

1. Open the Console Mobile Application.
2. From the tab menu at the bottom of your device, choose **Notifications**.
3. Select a notification in your inbox to view additional details.

Managing notifications

You can manage your notifications in any of the following ways:

Subscribing to a notification configuration

You can generate push notifications from existing notification configurations in your account by selecting them.

To subscribe to an existing notification configuration

1. In the Console Mobile Application, from the tab menu at the bottom of your device, choose **Notifications**.
2. Choose **Configurations**.
3. In the **All** tab, select notification configurations by choosing the plus sign (**+**).

Unsubscribing from a notification configuration

If you no longer wish to receive push notifications for an existing configuration, you can unsubscribe.

To unsubscribe from an existing notification configuration

1. In the Console Mobile Application, from the tab menu at the bottom of your device, choose **Notifications**.
2. Choose **Configurations**.
3. In the **Selected** tab, deselect notification configurations by choosing the green checkmark icon.

Deleting a notification configuration

If you no longer need a notification configuration, you can delete it.

> ⚠ **Warning**
>
> Deleting a notification configuration removes it from the account.

To delete a notification configuration

1. In the Console Mobile Application, from the tab menu at the bottom of your device, choose **Notifications**.
2. Choose **Configurations**.
3. Locate and choose the notification configuration.
4. Choose the vertical ellipsis icon.
5. Choose **Delete**.

> **Note**
>
> You can also manage your mobile device's push notifications from the AWS User Notifications console by adding your mobile device as a delivery channel, but this requires additional permissions. For more information, see Listing mobile devices as delivery channels.

IAM permissions for listing mobile devices as delivery channels

The AWS Console Mobile Application supports push notifications via AWS User Notifications. If you enable push notifications, the Console Mobile Application collects your device nickname (if applicable) to help identify your device. You can manage your mobile device's push notifications from the AWS User Notifications console by adding your device as a delivery channel. Delivery channels allow you to receive and view notifications in locations other than the AWS Management Console. You can remove your device as a delivery channel at any time.

You must have access to the `ListDeviceIdentities` and `GetDeviceIdentity` API actions to view your mobile device in the AWS User Notifications Console. The following sample policies show how to allow or deny permissions to these actions.

For more information about delivery channels, see Managing delivery channels in the *AWS User Notifications User Guide*.

Sample ListDeviceIdentities IAM policies

Allow ListDeviceIdentities

You can attach the following policy to your IAM identities. This policy allows access to `ListDeviceIdentities`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "consoleapp:ListDeviceIdentities"
            ],
```

```
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Deny ListDeviceIdentities

You can attach the following policy to your IAM identities. This policy denies access to `ListDeviceIdentities`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "consoleapp:ListDeviceIdentities"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Sample GetDeviceIdentity IAM policies

Allow GetDeviceIdentity

This policy allows a specific resource access to `GetDeviceIdentity`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "consoleapp:GetDeviceIdentity"
            ],
            "Resource": [
```

```
                "arn:aws:consoleapp::123456789012:device/2FQVtmveB13WEXAMPL3D3V1D/
identity/AIDACKCEVSQ6C2EXAMPLE",
            ]
        }
    ]
}
```

Deny GetDeviceIdentity

This policy denies a specific resource access to `GetDeviceIdentity`.

```
{
"Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "consoleapp:GetDeviceIdentity"
            ],
            "Resource": [
                "arn:aws:consoleapp::123456789012:device/2FQVtmveB13WEXAMPL3D3V1D/
identity/AIDACKCEVSQ6C2EXAMPLE",
            ]
        }
    ]
}
```

The following shows an example of the denial response:

```
{"message": "User: arn:aws:iam::123456789012:user/testUser-readOnly is
 not authorized to perform: consoleapp:GetDeviceIdentity on resource:
 arn:aws:consoleapp::123456789012:device/2FQVtmveB13WEXAMPL3D3V1D/identity/123456789012
 with an explicit deny"}
```

Supported AWS Regions and services

In this section, you'll learn which AWS Regions and services are supported by the Console Mobile Application.

Supported Regions

The Console Mobile Application supports the following Regions:

- US East (Ohio)
- US East (N. Virginia)
- US West (N. California)
- US West (Oregon)
- Asia Pacific (Mumbai)
- Asia Pacific (Osaka)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Canada (Central)
- Europe (Frankfurt)
- Europe (Ireland)
- Europe (London)
- Europe (Paris)
- Europe (Stockholm)
- South America (Sao Paulo)

Opt in Regions

Opt in Regions are not enabled by default. You must choose to enable them in the console before they can be used in the Console Mobile Application. The following opt in Regions are supported:

- Africa (Cape Town)
- Asia Pacific (Hong Kong)
- Asia Pacific (Hyderabad)
- Asia Pacific (Jakarta)
- Asia Pacific (Melbourne)
- Europe (Milan)
- Europe (Spain)
- Europe (Zurich)
- Middle East (Bahrain)
- Middle East (UAE)

Supported services

The Console Mobile Application supports the following AWS services:

- Amazon API Gateway
- AWS Artifact
- AWS Backup
- AWS Billing and Cost Management
- AWS CloudFormation
- AWS CloudShell
- AWS CloudTrail
- Amazon CloudWatch
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- AWS CodePipeline
- Amazon Cognito
- AWS Control Tower
- AWS Cost Explorer

- Amazon DynamoDB
- AWS Elastic Beanstalk
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Elastic Container Service (Amazon ECS)
- Amazon Elastic Kubernetes Service (Amazon EKS)
- Elastic Load Balancing
- IAM Identity Center
- AWS Identity and Access Management (IAM)
- AWS IoT
- AWS Lambda
- AWS OpsWorks
- AWS Organizations
- AWS Personal Health Dashboard
- Amazon Relational Database Service (Amazon RDS)
- Amazon Route 53
- AWS Secrets Manager
- AWS Security Hub
- Amazon Simple Queue Service
- Amazon Simple Storage Service (Amazon S3)
- AWS Step Functions
- AWS Systems Manager
- AWS User Notifications
- Amazon Virtual Private Cloud (Amazon VPC)

Note

The Console Mobile Application supports a select subset of features for the AWS services listed above. If you don't see a feature you want to use on the app, you can contact us. You can also leave feedback in the app by choosing the menu icon in the upper left, then choosing **Feedback**. Add your comments, optionally include logs, and then choose **Submit**.

If you use AWS Billing and Cost Management, note that you need to have API permissions to use that service on the mobile application. See the example IAM policy in Getting started with AWS Console Mobile Application.

Monitoring AWS Console Mobile Application

Monitoring is an important part of maintaining the reliability, availability, and performance of AWS Console Mobile Application and your other AWS solutions. AWS provides the following monitoring tools to watch the Console Mobile Application, report when something is wrong, and take automatic actions when appropriate:

- *AWS CloudTrail* captures API calls and related events made by or on behalf of your AWS account and delivers the log files to an Amazon S3 bucket that you specify. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred. For more information, see the AWS CloudTrail User Guide.

Logging DeviceIdentity API calls in AWS CloudTrail

Mobile devices using the Console Mobile Application can be configured as delivery channels for AWS User Notifications. This is done using the ListDeviceIdentities and GetDeviceIdentity APIs. These APIs are integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service on these APIs. CloudTrail captures API calls for ListDeviceIdentities and GetDeviceIdentity as events. The calls captured include calls from the the User Notifications console and code calls to the aforementioned API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for ListDeviceIdentities and GetDeviceIdentity. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to ListDeviceIdentities and GetDeviceIdentity, the IP address from which the request was made, who made the request, when it was made, and additional details. For more information, see Viewing Events with CloudTrail Event History.

To learn more about CloudTrail, including how to configure and enable it, see the AWS CloudTrail User Guide.

- Overview for creating a trail
- CloudTrail supported services and integrations
- Configuring Amazon SNS notifications for CloudTrail
- Receiving CloudTrail log files from multiple Regions
- Receiving CloudTrail log files from multiple accounts

DeviceIdentity API information in CloudTrail

The DeviceIdentity APIs support logging of the following actions as events in CloudTrail log files:

- ListDeviceIdentities
- GetDeviceIdentity

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the CloudTrail userIdentity element.

Understanding the Console Mobile Application log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the `ListDeviceIdentities` action.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:jdoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/user/jdoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
```

```
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111111112222:role/Admin",
                "accountId": "111111112222",
                "userName": "jdoe"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-10-24T04:13:00Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-10-24T04:13:35Z",
    "eventSource": "consoleapp.amazonaws.com",
    "eventName": "ListDeviceIdentities",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.3",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36",
    "requestParameters": {
        "maxResults": "100"
    },
    "responseElements": null,
    "requestID": "0def12ce-3020-4981-9346-5b5deb71eabb",
    "eventID": "3b5d601f-d1ef-4985-9ddd-5207065faf41",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111111112222",
    "eventCategory": "Management"
}
```

Security

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from data centers and network architectures that are built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security of the cloud and security in the cloud:

Security of the cloud – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS Compliance Programs. To learn about the compliance programs that apply to AWS Console Mobile Application, see AWS Services in Scope by Compliance Program.

Security in the cloud – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using Console Mobile Application. The following topics show you how to configure Console Mobile Application to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Console Mobile Application resources.

Topics

Data protection

The AWS shared responsibility model applies to data protection in the Console Mobile Application. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on

this infrastructure. This content includes the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the Data Privacy FAQ.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual users with AWS Identity and Access Management (IAM). That way each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. The Console Mobile Application does this for you, ensuring a secure connection between the application and your AWS resources.
- Set up API and user activity logging with AWS CloudTrail.
- Use AWS encryption solutions, along with all default security controls within AWS services.

We strongly recommend that you never put sensitive identifying information, such as your customers' account numbers, into free-form text fields such as a Name field. This includes when you work with Console Mobile Application or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into free form text fields for resource identifiers or similar items related to the management of AWS resources might get picked up for inclusion in diagnostic logs. When you provide a URL to an external server, don't include credentials information in the URL to validate your request to that server.

Data privacy

Diagnostics

By default, the AWS Console Mobile App stores and processes user data such as your device identification number and diagnostic information about the app's performance. Collected diagnostic information specifically includes: crash logs and performance data. This data helps AWS continuously improve the Console Mobile Application and your experience. Your diagnostic data isn't shared with any third parties, is anonymized, and is protected using sophisticated controls to prevent unauthorized access and misuse.

If you would like to turn off sharing this diagnostic information, you can do so by turning off sharing of this information in your device's settings. For more information see Share analytics, diagnostics, and usage information with Apple for iOS and Learn more about Google Play services for system diagnostics for Android.

Resilience in AWS Console Mobile Application

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see AWS Global Infrastructure.

For specific information about AWS Regions supported by the Console Mobile Application, see Supported regions.

Compliance validation for AWS Console Mobile Application

Third-party auditors assess the security and compliance of AWS Console Mobile Application as part of multiple AWS compliance programs. These include SOC, PCI, FedRAMP, HIPAA, and others.

For a list of AWS services in scope of specific compliance programs, see AWS Services in Scope by Compliance Program. For general information, see AWS Compliance Programs.

You can download third-party audit reports using AWS Artifact. For more information, see Downloading Reports in AWS Artifact.

Your compliance responsibility when using AWS services is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- Security and Compliance Quick Start Guides – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.
- Architecting for HIPAA Security and Compliance Whitepaper

> **Note**
>
> Not all services are compliant with HIPAA.

- AWS Compliance Resources – This collection of workbooks and guides might apply to your industry and location.
- Evaluating Resources with Rules in the *AWS Config Developer Guide* – The AWS Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- AWS Security Hub – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.

Security best practices for AWS Console Mobile Application

We recommend taking some basic security precautions when using the Console Mobile Application on your device. These measures will help protect your AWS account in the event that your device is lost or stolen.

- Make sure your device is protected by biometrics or a PIN code if your device allows.
- Enable biometrics on the Console Mobile Application.
- If your device is lost or stolen, perform a remote wipe by logging into your Apple or Google account on another device. This option should be available for most iOS and Android devices.

Troubleshooting

In this section, you'll find answers to some common questions and concerns.

Which password managers are supported by the Console Mobile Application?

The AWS Console Mobile Application supports password managers that are integrated with the mobile operating systems maintained by Apple (iOS) and Google (Android). For example, iCloud Passwords and Keychain, Google Chrome Password Manager, and Samsung Pass.

What hardware authenticators does the Console Mobile Application support for MFA?

The AWS Console Mobile Application supports all FIDO certified hardware authenticators, such as YubiKey, for MFA. For a complete list of FIDO certified hardware authenticators, see Fido Certified Products.

Which software authenticators does the AWS Console Mobile Application support for MFA?

The AWS Console Mobile Application supports software authenticators such as Google Authenticator, Microsoft Authenticator, and LastPass Authenticator. The AWS Console Mobile Application for iOS can also auto-fill MFA codes using the time-based one-time password (TOTP) feature built in to the in-app Safari browser used during sign in. For more information, see Multi-Factor Authentication (MFA) for IAM.

Can I use biometric authentication when signing into the AWS Console Mobile Application?

Yes. The mobile OS password managers that are supported by the AWS Console Mobile Application support the use of your mobile device's biometric authentication technology. If your mobile device

doesn't support biometric verification, your password manager may let you use the PIN that you set on your mobile device to verify your identity instead. If you don't have biometric verification or a device PIN enabled on your mobile device, then you can enter your AWS identity password to access your AWS resources within the AWS Console Mobile Application.

What if my organization's mobile device management policy doesn't allow the use of password managers or auto-fill?

If your organization doesn't allow the use of password managers or auto-fill, then must to sign in to your AWS identity in the AWS Console Mobile Application by entering your AWS identity's password.

How can I set and update my default identity?

If you only have one identity saved in the AWS Console Mobile Application, then it is automatically set as your default identity. If you save more than one identity in the AWS Console Mobile App, then you can modify your default identity from the Identities screen by choosing the **Actions** button in the upper right corner of the screen and then choosing the **Set a default identity** menu item. You can then set your default AWS identity by selecting its checkbox and choosing **Apply**. If you want to remove a default identity, unselect its checkbox and choose **Apply**.

I lost my device, what should I do?

If you lose your device, we recommend deactivating the user signed into the Console Mobile Application. We also recommend performing a remote wipe on your device.

Can I create resources within the app?

Currently, the only way to create resources from the app is to do so through the AWS CloudShell service using the AWS Command Line Interface (AWS CLI). Otherwise, you can view and sometimes modify resources within the app's graphical user interface, but you can't create resources through the graphical user interface.

Which CloudWatch dashboards can I access in the Console Mobile App?

You can search and view all CloudWatch custom dashboards that your AWS identity has permissions to access. CloudWatch automatic dashboards aren't currently supported in the AWS Console Mobile App.

Why am I being asked to log in again?

A session in the Console Mobile Application lasts 12 hours. After your session expires, you may need to log in again.

Can I leave feedback?

Yes. To leave feedback, open the app and choose the menu icon in the upper left, then choose **Feedback**. Add your comments, optionally include logs, and then choose **Submit**.

You can also provide feedback by contacting us.

Document history for AWS Console Mobile Application User Guide

The following table describes the document history for the AWS Console Mobile Application User Guide.

Change	Description	Date
Feature added	AWS CloudWatch dashboard support added.	March 28, 2024
Feature added	Amazon Q support added.	November 28, 2023
Feature added	Push notification support added.	April 20, 2023
Opt-in Regions added	Additional opt-in Region support added.	January 26, 2023
Service added	AWS CloudShell service added.	October 27, 2022
Feature added	The Recently Visited Services feature was added.	July 28, 2022
Region added	Support for the AWS Asia Pacific (Osaka) Region has been added.	April 9, 2021
Opt in Regions added	Four additional Regions are now supported. You must choose to enable them in the console before they can be used.	February 02, 2021
Public release	This is the initial public release of the AWS Console Mobile Application User Guide.	September 30, 2020

AWS Glossary

For the latest AWS terminology, see the AWS glossary in the *AWS Glossary Reference*.